



BGD e-GOV CIRT

TLP: CLEAR



CYBER THREAT ALERT

**Unresolved PHP Security
Exposures in Government,
Public and Private-Sector
Organizations in Bangladesh**



[THIS PAGE IS INTENTIONALLY LEFT BLANK]

BGD e-GOV CIRT

TLP: CLEAR**Distribution:** Public**Alert on:** Unresolved PHP Security Exposures in Government, Public and Private-Sector Organizations in Bangladesh**Advisory Type:** Vulnerability and Security Remediation Alert**Severity:** High — depending on the PHP version, patch status and exposure**Date:** 25 October 2026

Executive Summary

Through continuous monitoring by the **Cyber Threat Intelligence (CTI) Unit** of **BGD e-GOV CIRT**, several internet-facing web applications associated with government, public, and private organizations in Bangladesh have been identified as running outdated, potentially vulnerable, or end-of-life (EOL) PHP versions.

Despite previous notifications and security advisory, several concerned organizations have yet to respond or confirm the implementation of appropriate remediation measures. The continued exposure of these services without verified security updates may increase the risk of exploitation and compromise.

As highlighted in the BGD e-GOV CIRT advisory on *PHP2Shell: Critical Unauthenticated Remote Code Execution Vulnerabilities in PHP*, vulnerable PHP (dated 22 October 2026) deployments may be susceptible to remote code execution, potentially resulting in unauthorized access, sensitive data exposure, server compromise and service disruption.



Potential Security Risks

Organizations operating outdated or vulnerable PHP environments may face the following risks:

- **Remote Code Execution (RCE):** Potential execution of unauthorized commands on vulnerable servers.

- **Unauthorized Access:** Potential compromise of web applications and underlying systems.
- **Data Exposure:** Unauthorized access to sensitive organizational or user information.
- **Service Disruption:** Potential interruption of web services and business operations.
- **Further Compromise:** Potential use of compromised systems to facilitate additional malicious activities.

The actual risk depends on the PHP version, applicable security patches, deployment configuration, and exposure of the affected service. Identification of an outdated PHP version alone does not confirm successful exploitation.

Required Actions for Concerned Organizations

BGD e-GOV CIRT strongly urges all concerned organizations to take immediate responsibility for securing their internet-facing systems and implement the following measures:

- **Verify PHP Versions:** Identify the PHP runtime versions used by all public-facing web applications, servers, containers, and hosting environments.
- **Apply Security Updates:** Upgrade vulnerable PHP runtimes to the applicable security-fixed releases or install verified security-patched packages.
- **Replace EOL Versions:** Migrate unsupported PHP versions to actively supported releases with ongoing security updates.
- **Restrict Public Exposure:** Where immediate patching is not feasible, apply appropriate temporary access restrictions, such as VPN access, source-IP allow listing or removal of unnecessary public access.
- **Review Security Logs:** Investigate suspicious requests, unexpected processes, unauthorized file modifications and unusual outbound connections.
- **Coordinate with Hosting Providers:** Ensure that the underlying PHP runtime is updated, including in managed and shared hosting environments.

Temporary access restrictions may reduce exposure but do not replace the installation of appropriate security updates.

Responsibility and Compliance

Organizations are responsible for maintaining the security of their web applications and associated infrastructure, including systems hosted or managed by third-party service providers.

The continued failure to address known security exposures may leave critical services at increased risk of cyberattacks. All concerned organizations are therefore requested to treat this matter with the highest priority and ensure that appropriate technical and administrative actions are taken promptly.

Organizations that have already implemented remediation measures should verify the effective patch status of their production PHP runtimes.

BGD e-GOV CIRT

BGD e-GOV CIRT reiterates that maintaining secure and supported PHP environments is essential to protecting Bangladesh's government, public-sector and private-sector digital infrastructure.

All concerned organizations that have previously been notified but have not yet confirmed remediation are strongly urged to take immediate corrective action. Organizations should not delay remediation until a security incident occurs.

Reference:

BGD e-GOV CIRT, PHP2Shell: Critical Unauthenticated Remote Code Execution Vulnerabilities in PHP, dated 22 October 2026.

<https://www.cirt.gov.bd/advisories/php-oct-2026>



BGD e-GOV CIRT